REPORT

of the

Copy Protection Technical Working Group

June 21, 1996

AEI

The following firms and trade organizations provided input to this report and/or participated in the Spring '96 technical discussions:

Apple Computer, Inc.
Business Software Alliance
Compaq Computer Corporation
CCIA
Debevoise & Plimpton (for Sony)
Digimarc
Digital Equipment Corporation
Eastman Kodak Company
Electronic Commerce Technologies
Electronic Publishing Resources
Fujitsu, Ltd.
Fujitsu America
Hewlett-Packard Company
Hitachi, Ltd.
Hitachi America, Ltd.
Horizons Technology, Inc.
IBM
Information Technology Industry Council
Intel Corporation
Interactive Multimedia Association
ITA - Advanced Television Laboratory
Information Technology Industry Council
JVC
Macrovision
Matsushita Electric Industrial Co., Ltd.
MCA / Universal
McDermott, Will & Emery (for HRRC)
MGM / UA
Mitsubishi Electric Corporation
Microsoft
MPAA
Novell
Packard Bell
Paramount
Patapsco Designs, Inc.
Philips
Pioneer Electronic Corporation
Proskauer, Rose (for MPAA)
Recording Industry Association of America
Roberts & Co.
Sony Corporation
Sony Pictures Entertainment
Sun Corporation
Sun Microsystems
Thomson CE
Time Warner
Toshiba Corporation
Turner Entertainment
Twentieth Century Fox Film Corporation
Viacom / Paramount
The Walt Disney Company
Warner Bros.
Warner Bros. Records, Inc.
Warner Home Video
Weil, Gotshal & Manges (for Matsushita)
Wiley, Rein & Fielding (for CEMA)
Wunde, Diefenderfer Cannon
Xerox Corporation
Zenith

The group co-chairs are:

Alan E. Bell, PhD, IBM
Bob Lambert, The Walt Disney Co.
Bill Connolly, Consultant for Sony
Chris Cookson, Warner Bros.
David Stebbings, RIAA

REPORT
Copy Protection Technical Working Group
June 21, 1996

I. Introduction

As a result of the increasing capability to represent and distribute all types of content in digital form, there is considerable interest in copyright management schemes capable of protecting the legitimate rights of the owners of all forms of content and software in the electronic environment.

This report summarizes the main technical discussions of an ad-hoc group which met on four occasions between May 9 and May 30 1996 in order to evaluate the potential technological approaches to providing copy protection and rights management capabilities to linear motion picture content, as well as other forms of copyrighted content including sound recordings, in the PC environment, environments where a PC could be interposed, and the consumer electronics environment.

The main purpose of these discussions was to provide a neutral technical input to the plenary group, without prejudice to the outcome of further discussions regarding associated non-technical considerations. The plenary group is comprised of both policy and technical representatives of the member companies of the MPAA, CEMA, BSA, ITIC, RIAA and IMA.

In view of the limited time available to the technical group, the discussions were primarily focused on linear motion picture content and the copy protect scenarios related to the introduction of the DVD in particular. Even so, the discussions focused on overall evaluation of the merits and drawbacks of general classes of potential technological approaches, without drawing any final conclusions about the details of actual implementations or designs.

Although several broader issues were identified, they will require further activity beyond the work of this group in order to be addressed.

II. Objectives and scope

With the introduction of consumer digital devices capable of playing, transmitting and recording digital linear motion pictures, the capability for making and distributing high quality copies or re-transmissions of the original copyrighted material has increased. In the digital environment the degradations which are unavoidably associated with the equivalent analog processes are absent so this natural inhibition to copying is much reduced, even eliminated.

The overall objective of the group was to identify and evaluate technical approaches which could potentially be used to protect content in analog or digital form, delivered by direct electronic transmission or prerecorded media, against copying in analog or digital recorders or against re-transmissions in a form contrary to the usage conditions intended by the owner of the copyright, or contrary to legitimate and reasonable consumer usage. Analog to analog copy scenarios were not included within the group's agenda for discussion.

The scope of the technology evaluation included

1) the level of effectiveness of the copy protection for motion picture content and other forms of content such as sound recordings and software

2) whether the technology is "fail-safe", i.e. can remain effective in protecting the content, even in those devices that do not implement the scheme.

3) the impact on the intended usage of the content (i.e. there should be no noticeable degradation of the original material or of permissible copies)

4) the impact on cost

5) the impact on performance

6) the impact on product schedules

7) the extensibility of the approach with respect to potential future upgrades, including backward compatibility

8) the applicability to existing or legacy devices

III. Basic properties and desirable attributes

The desirable attributes of the copy protection scheme for linear motion picture and soun recordings content include

1) protection for digital linear motion pictures, including segments as small as single frames, and sound recordings including samples.

2) a level of protection that will prevent the average consumer from unlawfully making and/or distributing copies or re-transmissions, i.e. 'keep honest people honest'

3) capability to deal with three primary options for usage conditions, as well as a method for associating those options with the content in a persistent way,

a) copying is permitted
b) copying is not permitted
c) one generation only of copying is permitted

4) capability to address current and future classes of content sources and destinations, including

a) digital to digital
b) digital to analog
c) analog to digital

where the digital devices include dedicated, stand-alone consumer video recording and playback products in addition to general purpose digital recording and playback devices associated with computing systems. The analog devices include existing VHS, 8mm and other formats of consumer analog video recorders, as well as the analog interfaces to consumer digital video recorders. The digital and analog interfaces to computers are also included.

5) capability for application on an international basis

6) capability to offer a range of copy protection and rights management alternatives to the content owner, having various levels of cost, complexity and effectiveness.

7) capability to limit the potential exposure resulting from a breach in the system

From the viewpoint of consumer electronics hardware and computer systems manufacturers, the desirable attributes of the copy protect implementation include

1) acceptably low or insignificant impact on the cost, performance, manufacturability and availability of devices

2) compatibility with accepted standards and existing devices

3) compatibility with existing processes and architectures

4) upgrade capability with backward compatibility

5) broad applicability to all forms of content or software in the computer environment

6) applicability to prerecorded disc media of both the stamped and the directly written kind

7) capability to provide copy management of copyrighted material in both computer and consumer electronic environments

IV. Technical evaluations

A. General observations

The group reached an overall consensus on two principal recommendations which merit further investigation and evaluation in terms of specific implementation proposals to determine mutually acceptable and effective copy protection and management schemes

1) in the case of digital content information, the content itself should be protected prior to initial distribution by direct application of some combination of encryption and/or scrambling type encoding by the copyright owner. The advantage of such 'self-protected' content is that no special digital copy restrictions need be applied to the content while it exists in encrypted and/or scrambled form. The keys necessary to decrypt and/or de-scramble the content for display, copying or re-transmission purposes are only provided to devices when the usage is consistent with the defined conditions, whether these devices are part of the local system or connected remotely through a digital transmission interface.

2) the basic information concerning the usage conditions should be embedded within the active content data stream, even though for the purposes of some consumer electronic devices it may, in addition, be carried as associated data along with the content stream. The advantages of such 'self-describing' content having embedded control data, particularly in those environments which include computers, are that it

   a) ensures that the usage conditions are available to any transmission interface or recording device which bases compliant operation on detection of, and response to this information

   b) guarantees the transmission of the control information between the digital and/or analog input/output interfaces of computer systems. Since computer systems and processes preserve the active content data stream, no special actions would be required to assure transmission of the embedded control information.

Table 1 shows the group's evaluations of four general approaches to encryption based schemes.

Table 2 shows the group's evaluation of embedded data schemes for carrying the content usage conditions data, as compared to non-embedded schemes.

B. Specific environments considered

1) Digital to Digital

DVD will provide consumers access to high quality digital linear motion picture content, sound recordings and computer software, and requires the most immediate solution for copy protection. Of several schemes that were described, most favored those which included scrambling and/or encryption of the content directly on the DVDROM media in order to control unauthorized access. Example schemes based on encrypted and/or scrambled content were described by both IT and consumer electronics companies. Not only do such approaches provide protection to the content on the DVDROM media, but the content also remains protected even in those systems which did not implement copy protection, i.e. such schemes can be fail-safe. The effectiveness of the schemes, as well as their impact on the schedule and cost factors associated with the introduction of DVD products will, of course, depend on the final details of the chosen implementation as it is developed.

The use of encrypted content alone does not prevent the making of encrypted digital copies. Therefore, for DVD-R or DVD-RAM devices in particular, the overall copy protect and rights management scheme will require a method to allow playback of a copy by a DVD player or drive only when that copy complies with the usage conditions set forth by the content owner. Playback control schemes were described which were based on the method for key management, or through comparison between special (watermark) data embedded in the content and data physically embedded in the original ROM disc media, which is either not present, or has a different value in the recordable media blanks. Further study is required as to how such schemes could support one generation copying and serial copy management, and under what circumstances these features are required.

The group reviewed approaches to the secure delivery of digital content and rights management control information based on digital container technologies. In one scheme presented to the group the decryption keys, control information and content is placed in the same container and carried directly on the DVD media itself. The content is only decrypted when software on the computer or player determines that the usage conditions have been met. Altematively, the key management could be assigned to a remote trusted agent, and released to the player or drive only on completion of a specific transaction between the agency and the drive or end-user. Such approaches are capable of affording high levels of effectiveness in the future when the digital content is transmitted to the consumer by direct electronic means. In that case the key exchange transaction could be a natural component of the overall transaction. In the mean time, applicability of digital container technology to the distribution of content on DVDROM requires further study.

Representatives of the sound recording industry described copy management systems they recommend for sound recordings. These systems included copyright management using a bi-directional authorization system from source to end user, time windows, embedded signaling and recordable areas on stamped discs.

2) Digital to Analog

Two types of analog video outputs, in addition to optional audio outputs, may be present on a computer: RGB, and NTSC.

(a) The RGB output is necessary for output to the computer display and therefore is almost always present as part of the computer system. The precise definition of the RGB output signal is dependent on both the display parameters and computer systems' manufacturers specifications. In general, dedicated consumer video recorders do not accept RGB inputs so that, in order to make an analog copy from this interface, a format converter to NTSC, or other consumer recordable analog video format is required.

(b) The NTSC analog output is typically not present on the installed base of computers, however if an NTSC analog output is optionally present, then the output signal may be directly connected to a consumer video recorder. Depending on the overall evolution of applications for computer systems, the inclusion of an NTSC video output may become more prevalent in the future.

The existing base of analog consumer VCRs (i.e. VHS, 8mm and Beta, for example) presents an immediate capability to make analog copies from DVD or other digital source material via the NTSC video output. These analog consumer VCR machines have no ability to either detect or respond directly to information regarding usage conditions, whether directly embedded or transmitted in association with the content signal. As a result, copy protection in the analog consumer VCR domain must take the approach of rendering the copy unviewable, or at least extremely unsatisfactory during playback. Such approaches may generally be referred to as analog protection systems, or APS. The current method (developed by the Macrovision Corporation) works by using this kind of approach. By placing certain signal features into the vertical blanking interval and/or periodically modifying the color burst signal, the recording circuits of the VCR are disturbed in a way that results in a substandard recording being made to the cassette. These same features do not similarly upset the input circuits of television sets , so analog signals incorporating the APS eatures may remain viewable even when copy protected.

If analog protection signal features are applied to the analog video signals encoded on the NTSC video outputs of computers or format converters attached to the RGB outputs of computers, they would provide the equivalent level of protection against copies made to consumer analog VCRs as is currently experienced. Similarly, the absence of analog signal protection features will result in an NTSC video signal output which is unprotected and may be copied without technical impediments by a consumer analog VCR.

No presentations on potential approaches to providing APS on the RGB output were made to the group, and discussions concerning initial concepts were largely inconclusive in terms of identifying an effective and satisfactory approach.

3) Analog to Digital

The basis for copy protection with respect to stand-alone digital video recording devices consists of two main elements.

a) The control data expressing the content owners usage conditions is always associated with the content data. Embedding the control data into the active part of the content data ensures that from the computer system viewpoint the data is, by default, preserved through all normal processes which protect the content itself. The group also discussed the use of embedded data in the audio signal accompanying the linear motion picture to carry the usage conditions associated with the rights management.

b) Dedicated stand-alone digital video recording devices (such as the DVCR) which receive the content must detect and respond to the control data in a compliant fashion. Although DVCR products generally have implemented copy protection methods based on active response to control data, to date such data has not been embedded directly in the content. If the control data scheme is not of the embedded type, and if the digital output is to be communicated to such a dedicated stand-alone video recording device, then the associated control data would need to be applied at the appropriate digital output of the computer during the overall DVCR (or other) format encoding process, in a manner analogous to that described in section B.2) with respect to any analog protection signal features applied during the NTSC encoding process.

In order for the analog source data (or initially digital-to-analog converted source data) to be output as a converted-to-digital copy signal to be recorded by future recordable DVD media, there will need to be consumer-level access to DVD encoding capability in the computer system, including the capability for MPEG2 compression. In this circumstance, the combined effect of authentication via embedded data (or watermarks) and playback control methods, as mentioned above in the section on digital to digital, will provide a capability for copy protection of the analog source material.

No technical methods were found to prevent the copying of the (initially-analog-to-digital) converted video content to general purpose removable media digital storage devices (excluding the recordable DVD devices already discussed in the previous paragraph). However, the relatively low penetration of such devices, coupled with the relatively high cost for both media and drives significantly limits their utility to support copying of motion pictures in the consumer environment.

C. Recommended future activity for the technical group

The broad consideration and evaluation of the technological approaches which might form the basis for a mutually acceptable and reasonably effective copy protection scheme has now been completed by the technical group. The technical group recommends that the next phase consist of entering into more detailed and open technical discussions involving the development of specific proposals on the detailed specifications for copy protection. At that point, all parties can better evaluate the technical and economic viability of the proposed approaches described in this report. This work should focus at first on the near term issues involved in the DVD player and DVD-ROM areas, and then expand to cover all the relevant channels for the distribution and transmission of copyright content of all forms where rights management schemes are thought to be beneficial.

	Encrypt Content	Encrypt at Drive	Encrypt Content and Encrypt at Drive	Closed System	Comments
Domain	D-D	D-D	D-D	D-D	1. Need to protect both stamped and recorded content on DVD
Coverage Sources	DVDROM and Player	DVDROM and Player	DVDROM and Player	DVDROM and Player	
Capability (0,0) (1,0) (1,1)	 Y Y Y	 Y Y Y	 Y Y Y		1. Capability for SW backup maybe implemented via control data codes 2. Copy control of decrypted content requires either embedded or associated data
Content Unit	>1 frame	>1 frame	>1 frame	>1 frame	
Security Level	3 adds content protection on the media itself	3 assuming all drives are encryption enabled	3	3	0 = none 1 = average consumer 2 = hobbyist 3 = professional
Type of Secret	Each Master	Global (note 1)	Master (note 2)	Master (note 2)	1. Both drive and MPEG secrets require update 2. With private media key
Consequence of Breach	1 Title or Part of Title	All titles	1 Title or part of title	1 Title or Part of Title	I.e. Exposure to content owner
Availability	Design and Development	Design and Development	Design and Development	Design and Development	
Cost Impact Player ROM PC (note 1) Media	 Y Y (lower) Y Y (small, note 2)	 N Y (higher) Y N (none)	 Y Y (higher) Y Y (small, note 2)	 Y Y (much higher) Y (much higher) Y (small, note 2)	1. Depends on the encryption scheme 2. Content encryption engine amortized over many titles
Schedule Impact Player ROM PC Media	 Y Y (note 1) Y Y	 N Y (note 2) Y N	 Y Y Y Y	 Y Y Y Y	1. Needs key access method 2. Needs key access method plus encryption capability
Performance Impact Player ROM PC User	 note 1 note 1 Y note 2	 note 1 note 1 Y note 2	 note 1 note 1 Y note 2	 note 1 note 1 N note 2	1. Insignificant impact on the performance is a critical requirement 2. Must have high quality playback in all circumstances
Extendible Audio SW and Data	 Y Y	 Y Y	 Y Y	 Y N	
Implementation Microcode Drive HW Player HW PC SW PC HW	 Y Y (note 1) Y (note 1) Y (note 1) Y	 Y Y N Y (note 1) Y	 Y Y Y Y Y	 N N Y N N	1. Actual combination depends on details of implementation
Upgradable?	Y	Y	Y	Y	
Fail-safe?	Y	N	Y	Y	1. As defined in the body of the report
IP Status	TBD	TBD	TBD	TBD	
Backward compatibility Old drive with new media, note 1 New drive with old media, note 2	 N Y note 3	 Y Y note 3	 N Y note 3	 N Y note 3	1. Depends on degree of upgrade 2. Desirable not to obsolete old media with new drives, lasting value of content 3. Vulnerable to possession of clear Content and an Encryption Engine
Effectiveness with SW Implementation	Reduced	Reduced	Reduced	Reduced	

Table 1

Other comments:

1) Export/Import Law compliance required for encryption
2) Is there a distinction between shipping encrypted content versus encryption devices?
3) Implications of encryption approaches for archive content needs to be considered.

Table 2

Note:
The Something Very Simple (SVS) example is that concept which was presented by Apple during the meeting on 5/30/96. SVS consists primarily of incorporating two bits of information in line 22 of the analog video signal, which is normally hidden from view as a result of overscan. No active data hiding techniques were incorporated.

The CGMS example is that initially proposed by CEMA and MPAA. CGMS consists primarily of two bits of information carried along with, but separately from, the video content stream.

	Embedded Data For Example, SVS	Associated Data For Example CGMS
Domain	D-D, D-A, A-D	D-D, D-A, A-D
Coverage	Analog or Digital Inputs of DVCR	Analog or Digital Inputs of DVCR
Capability		
(0,0)	Y	Y
(1,0)	Y	Y
(1,1)	Y	Y
Extendible?	Y	Y
Content Unit	Frame	Field
Security Level	Low for SVS Watermark can improve tamper resistance	Low for CGMS
Consequence of Breach	Inappropriate response by recorder device	Inappropriate response by recorder device
Effect of breach	None for SVS Artifacts may result from watermark change or removal	None for CGMS
Availability	SVS needs design and development More information required about watermarking. Needs development and maybe research	CGMS needs design and development for the PC. Available in DVCR environment
Cost Impact		
DVCR	Y	N
Player	N (if no player response to data is req'd)	N
ROM	N	N
PC	N	N
Schedule Impact		
DVCR	Y (but cannot change product in the market)	N
Player	N (if no player response to data is req'd)	N
ROM	N	N
PC	N	N
Performance Impact		
DVCR	N	N
Player	N	N
ROM	N	N
PC	N	Y
Consumer	Small for SVS (visibility), reduced by data hiding	None for CGMS, small for APS
Extendible		
Audio	No for SVS Yes in general	No for CGMS. In general: No for D-A, A-D, Yes for D-D
SW and Data	No	No
Upgradable?	Y	No for CGMS, Yes in general
Fail-safe?	N	N
IP status	TBD	CGMS is proprietary but useable without a fee Macrovision APS is proprietary, licensed for a fee
Backward compatibility	Depends on the degree of change	Depends on the degree of change
Vulnerability	Same as CGMS Data hiding could be used to reduce vulnerability	Same as SVS
Other Comments	Passive/safe Embedded data can be used to provide CGMS/APS on output from the PC	Passive/fail

Attachments

The following are summaries which were received of some of the proposals which were presented to the group during the course of the series of four meetings. The are provided, as attachments to the main body of the report, in the form submitted and without editorial or other revisions by the co-chairs.

Further information is available by contacting one of the co-chairs.

DIGITAL TO DIGITAL COPY PROTECTION

Apple Computer
Paul Wehrenberg

ABSTRACT

Data Encryption and Decryption

The 'sine qua non' for a voluntary system of copy protection is encryption of the data to be protected, so that clear text does not appear on the media. In this proposal the main data stream is encrypted by segmenting sectors and scrambling the segments in sequential groups of sectors. For example, if 16 sectors (32 KB of user data) are segmented and the trailing segment of each sector randomly concatenated with a leading segment, 16 new 2KB blocks result out of 16! possible combinations. The information to correctly order these segments is contained in a 16 element (64 bit) scrambling vector, which is itself encrypted using a key which is hidden on the media. One nibble of the encrypted scrambling vector is placed in the header of each sector, creating no additional overhead if the reserved area is used. During playback, the encrypted scrambling vector is acquired from the headers, decrypted using the key from the media, the 16 sectors of user data are correctly reassembled, and the data used by the destination process. The scrambling scheme is designed to be computationally intensive to break if attacked as a jig saw puzzle, but easy to reorder if the key is available.

Key Placement and Exchange

During media manufacture one key or group of keys is placed on the media in a location or sub channel that is only accessible to the drive controller. It is not in an area that is addressable by logical block address (LBA). This key will be the message for a public key/private key transaction through the open computer system.

The drive controller is possessed of a public key and a private key, and has the capability of receiving another entity's public key. The drive can then encrypt a message using its private key and the received public key. This encrypted message can be requested by the operating system and passed to the owner of the non drive public key.

At startup the DVD-ROM device driver requests the Operating System to provide certified public keys of legitimate destination processes (H/W or S/W) running in the system. The driver for the destination process also requests the Operating System to provide the certified public key of the drive. Performing this function only at startup limits the opening for a 'spoofer' process to establish a session with the drive and obtain the media key.

The destination process then uses its own private key and the drive's public key to decrypt the received message. As noted above, the message is the key(s) on the media.

The transaction described above uses very robust encryption which may be computationally intensive. However the size of the message is relatively small and the transaction is done infrequently, in some instances only at startup.

Summary of a Copy Protection Scheme for DVD
Hewlett Packard Labs, 17th June, 1996
Josh Hogan

This Copy Protection Scheme is based on encoding a decryption key or an identification number in the channel coded bit stream, in a manner that will not be transferred by direct copying of the files on a disc.

The DVD encoder will include a state machine that will have the ability to select more than one codeword to represent at least some symbols. Such an encoder can correctly represent data symbol sequences with multiple bit pattern strings, all of which are valid. This choice of bit patterns is intended to allow the low frequency content of the bit stream to be minimized, but could also be used for encoding decryption keys or identification numbers onto the bit stream. Furthermore, the nature of the encoder allows a small number of codeword choices to have a dramatic effect on the encoded bit stream. In particular the statistics of the different runs of zeros in the bit stream can vary for different encoding of the same user data. The decryption key is derived from the bit stream by accumulating the run length statistics of a specified 32kbyte data block and then decoding these statistics according to a criteria set contained on the disc.

When a movie disc is played or a software package is installed from a disc, the first step of the play or installation routine, is to instruct the player to access the relevant 32kbyte blocks, accumulate the run length statistics of these blocks and generate the decryption key from the criteria also contained on the disc. It then instructs the player to read and decrypt the encrypted 32kbyte data blocks (or to decrypt blocks, or sections of blocks, on the fly).

If a copy of the disc is made, however, the new disc will have a bit stream with different run length statistics and so, will no longer contain the ability to generate the correct decryption key.

A valuable aspect of this approach to "hiding" the key on the disc is that in order to make an unauthorized copy of the disc, both software and hardware hacking have to occur. Specifically the install or play software routine must be analyzed in order to determine which 32kbyte data blocks contain the decryption keys and the bit stream endocing must be analyzed in order to determine the original channel coding that must be recreated to yield the keys.

This scheme for hiding the keys on the disc can be used with many different types of actual encryption or scrambling implementations. It forms one important element in an overall solution. This approach to that important element of any protection scheme (i.e. how to hide the key on the disc), is also applicable to both stamped and written discs.

Tel 415 857 7335 FAX 415 857 7724
E-Mail josh_hogan@hp1900.hp.com

Synopsis of Proposals Submitted by Matsushita Electric Industrial Co., Ltd.

In the interest of furthering the technical discussions on digital to digital copy protection Matsushita Electric has put forward two basic proposals: A) "Content Scrambled DVD", and B) "Bus Authentication and Encryption" using different encryption, authentication, and placement strategies, which it feels address in a practical and timely way the diverse concerns of consumer electronics, movie, and information technology industries. The two approaches summarized below can be used separately or in combination to provide different levels of effectiveness and "fail-safe" dependent on different legislative regimes. In PC environments, the proposal "B)" should be used in combination with the proposal "A)".

A) "Content Scrambled DVD"

Under this proposal the DVD content would be scrambled (encrypted) prior to producing a master which is then used to replicate separate discs during manufacturing. Data can be scrambled on a sector by sector basis with certain disc navigation information left in the clear for better control during playback. The chosen scrambling method provides protection equally well for all forms of content (movie, audio, or other ROM type data). For best security and speed descrambling would be done on chip before the audio

and video decoding process. Various key management and associated authentication strategies are possible to implement resulting in different levels of simplicity, effectiveness, and vulnerability. One method uses a "encrypted disckey" stored in the hidden lead-in area (key changed for each master), as well as separate encrypted keys for each title which are stored in the sector header area. An important feature of this approach is that a stand-alone DVD movie player can be designed which uses only descrambling/decryption, and thus easily meets export regulations.

B) "Bus Authentication and Encryption"

In this proposal an encryption process would be included in the DVD-ROM drive output circuitry connected to the computer bus, and complementary decryption would then be performed at the decoder also attached to the bus. Keys would be transmitted in a secure form over the standard bus from the DVD-ROM drive to the audio and video decoder as a result of a two stage bi-directional authentication process. For this purpose time varying key sharing should be used. Because this approach does not depend on the content of the source being encrypted, when incorporated in the computer bus interface it can provide security during transmissions within the computer for a wide variety of internal and externally attached digital media and electronic delivery services.

InterTrust™ Copy Protection and Rights Management for Consumer Appliances and Computers

Executive Summary

Presented By
Electronic Publishing Resources, Inc.
460 Oakmead Parkway
Sunnyvale, CA 94086
408-774-6100

Detailed EPR Contact Information

For additional technical information regarding InterTrust Commerce Architecture™ and DVD-related copy protection, please contact Mr. David Van Wie, SVP Research, V: 408-774-6100, F: 408-774-6144, E-mail: dvw@epr.com.

For additional business information regarding InterTrust Commerce Architecture and DVD-related copy protection, please contact Robert Weber, SVP Business and Technology Strategy, 408-774-, 6103, F: 408-774-6144, E-mail: weber@epr.com.

For InterTrust product information, please contact Michelle Arden, VP Marketing and Business Development, 408-774-6136, F: 408-774-6144, E-mail: arden@epr.com.

Electronic Publishing Resources, Inc., 460 Oakmead Parkway, Sunnyvale, CA 94086, 408-774-6100

This brief paper summarizes an important set of technologies for copy protection and rights management that, if implemented by the consumer electronics industry, will preserve vital options for rightsholders over the next several years. At the same time, the technologies presented here provide a key bridge between consumer appliances and computers of all sizes and capabilities.

The solution presented in this paper is based on research conducted by Electronic Publishing Resources and its principal scientists stretching back more than 10 years. The results of this effort include technologies for secure electronic commerce, copyright protection, and rights management for both the consumer and computer markets. We refer to the overall technology as the InterTrust Commerce Architecture™. The first end to end prototypes of this approach were completed in 1994, and EPR will ship its first commercial products based on this architecture later in 1996.

InterTrust™—in conjunction with other technologies for protecting analog video and tamper-resistant hardware and software—solves the copy protection problem in both key markets. Studios and other rightsholders are understandably concerned with both copy protection and ensuring the integrity of their works in digital format. An InterTrust-based solution not only solves both problems, but lays the foundation for other business models that may become important in the near future.

InterTrust is a modular, tamper-resistant, software technology that provides protection for digital properties of all kinds, including film, music, image, multimedia, software, and text. In conjunction with cost-effective tamper-resistant hardware, the level of protection is quite substantial. Encryption will be useful in protecting intellectual properties in digital format regardless of media. With respect to DVD, the key purpose of encryption is to enforce the use of a copy control and rights management system in order to ensure that only authorized people can use the content, and then only in authorized ways.

EPR has devised an encryption-based copy protection method with more than adequate strength that we believe meets existing U.S. export requirements. But encryption is a means rather than an end. The more difficult issue is to devise methods that ensure, to the maximum extent practical, that only authorized devices and users can decrypt the protected content. Current computer security and cryptographic methods can make it very difficult, but not completely impossible, for someone to compromise the protected digital property. However, these methods raise the bar sufficiently high that only technically sophisticated opponents bent on mischief can defeat the security system.

The best solution for effectively managing digital properties has two additional elements. The first key idea is that hardware and software be made "tamper-resistant." In the case of hardware, this means that some of the device control logic and information such as encryption keys and software could be put on a single chip, or inside a tamper resistant enclosure. The protected information would be used in accessing the content. In some devices, the information on the chip could not be easily accessed. In other devices, the act of accessing this information would destroy the chip itself. In the case of software, we have created a "self protecting" software container that is highly resistant to attacks by unauthorized devices and people, and especially so if used in conjunction with tamper-resistant hardware. EPR refers to a software container designed to work with InterTrust as a DigiBox™.

The second key idea is that one can associate one or more sets of business rules with a digital property such as a film or music track. Existing analog copy protection methods for VCRs already have a single, fixed rule. The business rule is "don't make a good copy of this property." The proposed DVD rules extend this to limit copying to a single generation, as well as to permit unlimited copying. Encrypted digital properties, together with business rules concerning the numbers of permitted copies, can be placed into in a tamper-resistant software "container" stored on DVD media. The rules can then be enforced by consumer appliances. These same rules, or more flexible rules, can also be enforced by computer devices.

The software container can also store certain content in unencrypted form. For example, movie or music titles, copyright statements, audio samples, trailers, and advertising can be stored unencrypted and displayed by any appropriate application or device. At the same time, valuable digital properties of all kinds—film, video, image, text, software, and multimedia—can be stored encrypted and accessed only by authorized devices and applications and only under rightsholder-approved circumstances.

Another important idea is that multiple sets of rules can be stored in the same DigiBox on the DVD disk. The InterTrust software then applies the appropriate rules depending on whether the movie is played by a consumer appliance or computer. Some usage rules may apply when the property is played by a consumer device and different rules may apply when played by a computer. This capability can also be used to provide users, particularly computer users, with choices about the set of rules that will apply. For example, a rightsholder may offer people using computers both a pay per use and a one time fee model by including two rule sets for computer users.

The choice of rules is completely up to the rightsholders. For example, film rightsholders may wish to limit copying and also ensure that excerpts are not taken from their content, regardless of the context in which the property is played. Alternatively, rightsholders of sound recordings may wish to enable excerpts of no more than 20 seconds, and that these excerpts are not used to construct a new commercial work without permission.

In a digital consumer appliance, these rules can be enforced, provided a few additions are made to the microprocessor (~5k gates), and provided some ROM or flash memory[1] is made available to hold the necessary software. We believe that these additions will not add appreciable cost to the device. Devices can also be produced without InterTrust capability and outfitted with a socket to receive these capabilities in a field upgrade.

In addition, each ROM (or flash memory) can contain a digital document or "certificate" that uniquely identifies that particular appliance. The rules for a consumer appliance can ensure that a copy of a digital property is sent to another digital device only in encrypted form and only inside a new DigiBox. The DigiBox may also carry with it new rules appropriate for a copy, rather than the original rules. The sending consumer appliance may also put the unique identifier of the receiving device in the same secure container. Consequently, the new rules will ensure that the copy will be playable only on the intended receiving device.

The new rules can ensure that no additional copies are created. If the InterTrust software on a consumer appliance detects that a digital property is about to be played on a device other than the one it was intended for, it will to refuse to play that copy (if desired).

The same restrictions that apply to a consumer appliance can be enforced on an InterTrust-aware computer. In the above example, the rules could specify not to play this film on anything but a consumer appliance, or enforce the same rules on a computer. Alternatively, these same powerful capabilities could be used to specify different usage rules and payment schemes that would apply when played on the computer, based on the rightsholder's business model.

No backchannel is required for any of the models presented here, however, when backchannels are present—for example, in settop boxes with bi-directional communications or computers attached to networks—it is easy to independently deliver new rules for a given property. These new rules may specify discounts, time-limited sales, advertising subsidies, new general prices and so on. As noted earlier, determination of these independently delivered rules is entirely up to rightsholders.

The solution to universal copy protection and rights management advocated here provides the cost-effective copy protection that rightsholders desire now, while at the same time laying a foundation for flexibility in the unforeseeable future. From the beginning, EPR designed InterTrust to provide rightsholders with the powerful control capabilities they desire together with enormous flexibility regarding the rules for copy protection, content distribution, and pricing models.

[1] Flash memory (programmable memory), rather than ROM, may turn out to be the better solution to firmware because of its flexibility. The basic rationale is that rights management (indeed, all functions of the player) may change over time. The second rationale is that experience has shown that firmware bugs can undermine adoption of otherwise great technology. The third is that internationalization may require different rights management decision-making (e.g. Japan does not recognize "backup rights" in the same way that the US does. Therefore, it may make sense to implement the rules governing copy in a different way. For example, the “"no copy" rule in the US may actually be implemented as "one copy with a watermark").

Report of the Policy Group
June 21, 1996

Over the past weeks, the policy group has held 11 meetings. Attending have been representatives from: the BSA, ITI, RIAA, MPAA, CEMA and HRRC, and persons from member companies.

Representatives of ITI/BSA, CEMA/HRRC and MPAA have each tabled exploratory discussion drafts based on, or utilizing the concepts of anti-circumvention in conjunction with the introduction of digital video technologies. In addition, all parties, including RIAA, have amplified and clarified their respective key policy considerations (not limited to the circumvention issue) to be weighed in making decisions about specific technical and legislative proposals. Finally, each of the parties reaffirmed its commitment to finding the necessary ways and means to be supportive of the introduction of DVD technologies to the marketplace.

There is broad agreement within the policy group that assuring compliance with copy protection systems requires legislation. There is further agreement that such legislation needs to be based on making it illicit to circumvent, and/or fail to fully implement, certain kinds of copy-protection systems. The policy group also agreed that decisions on policy issues would have to fully take into account further information on available technological solutions.

The IT industry has proposed a two pronged approach to the issue of circumvention: 1) Prior to initial distribution of a copyrighted work, the content may be protected by direct application of an effective copy protection system, or a combination of such systems. 2) An obligation not to interfere with all, or any part, of such protection system(s), so long as the protection system(s) is adequately specified through an industry-led voluntary standards setting process, and it is widely implemented in respect of works intended for a specified class of devices.

Counsel for the motion picture industry has suggested for discussion an anti-circumvention model which would make it illegal to sell tools, or otherwise assist or engage in, circumvention of copy protection systems. To be protected under this model, such copy protection systems would have to be specified or described through a "qualified voluntary standard," a concept which requires definition, and the possibility exists that such standards may, in certain cases, have to be established through law or regulation. MPAA would have such standards and establishment apply to D-A and A-D, as well as D-D, copying, at final and intermediate stages, and to back to back and transmission contexts.

A counsel for the consumer electronics industry has tabled for discussion a model that includes an anti-circumvention provision. This model defines "circumvention" in the context of obligations on makers and distributors of devices with respect to (1) copy control technology applied to signals also protected by encryption or scrambling, and (2) copy control technology existing or applied after decryption/descrambling or in the absence of encryption or scrambling. It would provide an antitrust exemption for private sector agreement on a system or systems to be officially adopted. It would also include provisions for the points deemed essential by CEMA and agreed to by MPAA in the context of their draft legislative proposal.

While both MPAA and CEMA have been willing in good faith to discuss anticircumvention-based ideas and proposals of the sort hypothesized by counsel, they have also wished for the approach set forth in their mutually agreed draft legislative proposal to remain open for consideration, in whole or in part.

Each of the parties also clarified their positions on their key policy considerations.

The motion picture industry articulated two considerations: preventing or inhibiting copying in the various circumstances where such copying might occur; and, ensuring compliance.

CEMA enumerated eight such considerations: the need for technical systems to be sufficiently specific that manufacturers would not be inadvertently liable for failure to comply; preservation of consumers' rights regarding copying; relieving manufacturers of products covered by the legislation of exposure to suit for copyright infringement; relieving consumers of exposure to suit for private, non-commercial copying; ensuring technological compatibility; ensuring the availability of technology needed to comply with and/or implement copy protection systems with any technology royalty obligations assumed by the copyright owners in aid of whose rights the technology is being deployed; special rules for professional devices; and, tailoring of remedies for violations, including avoidance of multiple actions for the same conduct. CEMA is generally concerned as to the level of expense and burden on innovation that any solution might impose on consumer electronics or other devices.

The RIAA agrees with the MPAA that control over copying in the digital to digital environment (including through the intermediate analog loop when technologically feasible) must be a central feature of any solution. For sound recordings, this includes in particular the application of copy controls from "un-encrypted" but copyright-coded digital sources such as existing CD's, as well as from all forms of digital transmissions from a digital source. While

RIAA continues to have concerns about digital copying of analog sources, and analog copying of digital sources, RIAA has not proposed that any contemplated legislation or technical solution specifically deal with these issues (other than the intermediate analog loop referred to earlier in the D-D chain). This could be achieved either by drafting a comprehensive anti-circumvention provision broad enough to require devices to respond to embedded copyright management information, or by mandating particular standards to be incorporated into any device capable of recording protected copyrighted materials.

The IT industry presented two policy considerations: achieving results which could be predictably implemented by the IT industry; and establishing the needed technological standards through industry led voluntary efforts. The IT industries also expressed a readiness to address digital to digital copying threats, and to explore fully all other possibilities, so long as solutions can be developed consistent with the IT industry's policy goals, and the technology evaluation goals enumerated in the engineers' report.

Agenda for June 21 DVD Meeting

1. Report by the engineering group

2. Report by the policy group

3. Discussion of issues not addressed by the reports

4. Discussion of next steps